COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-2706
PHONE: (213) 974-8301 FAX: (213) 626-5427

WENDY L. WATANABE
ACTING AUDITOR-CONTROLLER

ASST. AUDITOR-CONTROLLERS
ROBERT A. DAVIS
JOHN NAMO
MARIA M. OMS

October 24, 2008

TO: Supervisor Yvonne B. Burke, Chair
Supervisor Gloria Molina
Supervisor Zev Yaroslavsky
Supervisor Don Knabe
Supervisor Michael D. Antonovich

FROM: Wendy L. Watanabe
Acting Auditor-Controller

SUBJECT: **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) ANNUAL STATUS REPORT**

This is to provide your Board with a status report on the County's Health Insurance Portability and Accountability Act (HIPAA) program. As you know, the Auditor-Controller is responsible for overseeing and auditing County covered departments' compliance with the HIPAA Privacy Rule, which became effective on April 14, 2003. The Chief Information Office (CIO) is responsible for the HIPAA Security Rule, which became effective April 20, 2005.

Under the HIPAA regulations, the County declared itself a hybrid covered entity and identified five covered health care departments that must implement and comply with the provisions of HIPAA. The covered departments are:

- Department of Health Services (DHS)
- Department of Public Health (DPH)
- Department of Mental Health (DMH)
- Department of Probation (Kirby Center only)
- Sheriff's Department (Medical Services Bureau Pharmacy only)

The following is a summary of the County's HIPAA Privacy Rule program, audit activities, and compliance issues.

HIPAA Annual Self-Certification Program

The Auditor-Controller Chief HIPAA Privacy Officer (AC-CPO) is responsible for providing guidance to the five covered departments, performing HIPAA compliance reviews, and responding to complaints and queries from the U.S. Department of Health and Human Services Office for Civil Rights (OCR). The AC-CPO investigates and responds to complaints filed by patients or County workforce members, oversees the covered departments' adherence to the HIPAA regulations, and updates policies and procedures as laws change.

Within the noted covered departments, there are many facilities with auditable subunits that require periodic review. Consequently, the AC-CPO developed an Annual Self-Certification Program (SCP) with a manual and pre-designed certification form for covered departments to complete and return for the AC-CPO's final review.

On August 14, 2007, former Auditor-Controller J. Tyler McCauley issued the SCP to the DHS, DPH, and DMH department heads. The AC-CPO then met with each department's privacy officer and requested the SCP be completed by September 1, 2008. DHS completed and submitted both privacy and security portions of the SCP within the required time frame. DMH submitted the Privacy Rule portion before the due date but required an extension to submit the Security Rule portion on October 10, 2008. DPH submitted the Privacy Rule portion before the due date and obtained an extension for the Security Rule portion to October 24, 2008. DPH is assessing their entire IT infrastructure for compliance with County and Department Information Security Policies, and internal security controls as required by HIPAA and other regulations.

The AC-CPO and the CIO are currently reviewing, assessing, and compiling the SCP information and will prepare a separate analysis by January 31, 2009.

Department of Public Health's Appointment of a Privacy Officer

In July 2008, DPH appointed Deborah Hooper as their privacy officer. Since Ms. Hooper's appointment, DPH has demonstrated a stronger commitment to deliver services to its patients and clients mindful of the HIPAA Privacy Rule standards. Ms. Hooper works closely with the AC-CPO to correct weaknesses and deficiencies within the DPH HIPAA program, and she was instrumental in developing a DPH taskforce to update their HIPAA Privacy Rule policies and procedures. We will continue to assist DPH with their efforts and will participate on their taskforce. DPH executive management is also actively involved with their privacy program and they periodically request the AC-CPO provide them with performance measures. We will encourage the DPH Information Systems staff to complete the HIPAA Security Rule sections of the SCP.

Department of Health Services

The DHS HIPAA program is staffed with a privacy officer, a compliance officer, and a security officer. During this past year, the security officer has been responsive to Security Rule issues and has proficiently communicated security breaches involving PHI to the AC-CPO. However, recent audits show the privacy and compliance officers are not routinely and timely reporting privacy complaints to the AC-CPO; additionally, we discovered that supervision and documentation of their HIPAA training program needs improvement at certain facilities.

On October 8, 2008, the AC-CPO met with DHS' executive management and HIPAA program staff to discuss several key issues including improving and increasing the flow of compliance program issues and information to the AC-CPO, their complaint process, and their privacy training program. Overall, the meeting was positive and the AC-CPO was reassured by their executive management and privacy officer that they are committed to the HIPAA program. DHS' privacy officer further agreed to improve communications with, and include the AC-CPO on future related taskforces, as appropriate.

In the following months, we will closely monitor the DHS HIPAA program to ensure compliance with the regulations and to assess whether their HIPAA program has sufficient resources to carry out their responsibilities. The pressure for DHS to improve its privacy program is particularly relevant now as new privacy laws become effective on January 1, 2009. These are discussed below.

HIPAA Privacy Complaints

The AC-CPO is responsible for receiving, documenting, and investigating complaints against the covered departments. From January 1, 2008 to August 31, 2008, the Auditor-Controller's HIPAA Hotline received twenty valid complaints. Of the twenty complaints received, four were OCR cases. The most common complaints involve allegations that County employees either improperly disclosed protected health information (PHI) or denied patients access to their medical records. To ensure that employee's understand patients' rights, the AC-CPO encourages departments to provide ongoing training on related policies and procedures. We also advise the departments to educate key staff on the County's right to deny their patients' access to medical records under limited circumstances, and in response to inquiries from law enforcement. The AC-CPO provides training to management and staff on HIPAA regulations and County policy, as needed. Our training also covers regulations and policies that prohibit intimidating and retaliatory acts against an individual who files a complaint.

HIPAA Privacy Reviews

From January 1, 2008 to August 31, 2008, the AC-CPO and our HIPAA Compliance Unit conducted reviews at LAC+USC Medical Center's Medical Records Unit, High Desert Glenchur Clinic, Compton Mental Health Center, Hollywood Mental Health Center, Lancaster Mental Health Center, Downtown Mental Health Clinic, Antelope Valley Public Health Center, Palmdale Nurse Family Partnership Program, and Whittier Public Health Center.

These reviews exposed infractions and observable noncompliance with the HIPAA regulations and departmental policies and procedures. The most common and reoccurring noncompliance issues relate to the Notices of Privacy Practices (NPP). A covered department that has a direct treatment relationship with an individual must provide the NPP upon initial service delivery. The NPP must be available at the facility for individuals to request and take with them. Covered departments must post their NPPs at their facilities in a clear and prominent location. The following are two examples of NPP infractions:

- The DHS Antelope Valley Health Center did not post their NPPs, as required. Subsequent to our audit, DHS posted the notice.

- The DPH facilities did not post the NPPs in any of their facilities reviewed during this reporting period. DPH has since made an effort to correct this infraction.

Upon finding any violation, the AC-CPO works with departmental management to take corrective action. Currently, the AC-CPO is working with DPH in evaluating their facilities to comply with the regulations, specifically, with the NPPs.

Training Program

Covered departments must train all members of its workforce on policies and procedures related to PHI and required by the HIPAA Rules to the extent necessary and appropriate for its workforce to carry out their functions. Covered and Memorandum of Understanding (MOU) departments receive online HIPAA training from Health Care Compliance Strategies, Inc. (HCCS). In addition, departments are required to train their workforce members on State privacy regulations and County and departmental privacy and security policies and procedures. In the months ahead, the AC-CPO will be meeting with and auditing the covered departments to ensure that workforce members are receiving consistent and appropriate training, the training materials are comprehensive, training is documented, and workforce members have access to the training.

DMH, DPH, and the Sheriff's Medical Bureau have central training coordinators that monitor and train their workforce on HIPAA departmental policies and procedures. The DHS HIPAA training is decentralized and conducted at the facility level.

Learning Management System

On July 1, 2008, the HCCS online training program migrated to the County's Learning Management System (LMS). Unfortunately, the LMS HIPAA training program is currently experiencing problems which the Internal Services Department, Department of Human Resources, and the CIO are in the process of correcting. The AC-CPO will work with all covered and MOU departments to encourage training for all current and new employees when the LMS HIPAA training becomes available. The advantages of the LMS program include uniform training of all workforce members, ability to generate reports in a timely manner, and ability to maintain transcript data in one location. Transcript information will follow employees throughout their County careers, and managers can monitor the scope and level of training attained by their staff. Each covered department's policy states that training will occur within thirty days of hiring the employee. Through the LMS, training coordinators can assess their department's overall level of compliance with the HIPAA regulations.

Because current LMS HIPAA training only covers federal law, departments must develop and present training relative to County and departmental privacy policies and procedures. The AC-CPO will work with the covered departments' privacy officers to develop training materials that incorporate relevant County and departmental policies and State privacy laws into the LMS HIPAA training program.

Enforcement and Penalties for Noncompliance

The Center for Medicare & Medicaid Services (CMS) enforces the HIPAA Security Rule while OCR enforces the HIPAA Privacy Rule. CMS and OCR standards for safeguarding PHI and protecting the privacy of individually identifiable health information are periodically modified. For example, OCR recently modified the standards that heighten penalties for retaliation, and how health care providers can communicate and share PHI with a patient's family. As a result, revisions to the covered entities' policies and procedures will be made to reflect these changes.

Generally, when OCR determines noncompliance with the regulations, they first request that the covered entity bring their operation into compliance. In certain circumstances, OCR may provide technical support in their efforts to help covered entities voluntarily comply with the Privacy Rule. Covered entities that fail to comply with the standards are subject to civil penalties or criminal prosecution. Since the implementation of HIPAA, the AC-CPO has responded to several OCR investigations and no penalties or fines have been issued to the County for noncompliance.

HIPAA Privacy and Security Rule Breaches and Investigations

The Privacy and Security Rules require that covered departments implement mandatory and reasonable safeguards in their programs to protect the confidentiality, integrity, and availability of PHI maintained electronically or in hard copy format. The CIO notifies your Board of any security breach, which includes PHI. If there is a security breach, the AC-CPO works with the department on mitigating any potential harmful effect on the client or the County. The department or the AC-CPO notifies consumers and appropriate State or federal agencies of the breach, and takes measures to ensure the breach does not occur again. Three examples of privacy and security breaches and our mitigation efforts are noted below:

1. On February 1, 2008, thieves broke into the Palmdale Nurse Family and Practitioners' (PNFP) office and took two County desktop computers. One of the stolen computers contained PHI that was not encrypted, but was password protected. HIPAA regulations mandate that covered entities have a contingency plan if PHI is lost, stolen, or destroyed. On March 18, 2008, the AC-CPO and DPH's Compliance Division conducted an audit of the PNFP operations. Our findings showed that the desktop computers were not connected to the network and the hard copy records were kept in various unauthorized areas outside the facility. Thus, DPH was not in compliance with the element of creating a retrievable, exact copy of electronic PHI medical records. Subsequent to the audit, DPH connected the PNFP office to their network, and the AC-CPO trained PNFP staff and management on the regulations of safeguarding PHI.

2. On another occasion, the DHS Audit and Compliance Division notified the AC-CPO that a Harbor-UCLA doctor's personal data assistant (PDA) containing patient information was stolen. The PDA was not encrypted. Per HIPAA regulations and Board policy, departments must have policies and procedures that govern the movement of portable media devices containing PHI. Board policy also requires that management approve the downloading of personal or confidential information to portable devices and the information be encrypted regardless of the type of portable device.

   We advised the DHS Audit and Compliance Division to notify patients who would be at risk of identity theft or whose medical information would be at risk of modification or theft. We further advised DHS to record this incident in each patient's Accounting of Disclosures' log located in each patient's medical record. Harbor-UCLA notified at risk patients in writing that their medical information may have been compromised due to a lost PDA by a clinic staff. Information about identity theft was included in the notification. DHS management counseled the physician on DHS' Acceptable Use for County Information Systems' policy.

3. In our third example, OCR notified the AC-CPO that they received a complaint against Compton Mental Health Center (CMHC) alleging that a therapist wrongfully disclosed patient information to another patient.

   CMHC provides crisis intervention, case management, life support and interim funding, community health promotion, vocational, socialization, and other rehabilitation services to the southern County communities. DMH stated that because of these types of services and in conjunction with group sessions, patients share confidential information with other program participants. Participants in group sessions are aware that confidential information is shared and each participant signs a consent and confidentiality form prior to participation. Although we found no HIPAA violation, we recommended that the consent form be more descriptive and provide patients with an opportunity to request that certain information about them not be disclosed. We are working with County Counsel and DMH to develop a comprehensive authorization form.

State Legislation

On September 30, 2008, AB 211 and SB 541 became law, which enables the State to impose fines on licensed hospitals, facilities, and others that wrongfully breach the privacy of patients' medical records. In conjunction with this law, a new State Office of Health Information Integrity was created. This office has the power to review security plans and violations of patient privacy, and impose fines up to $250,000. The laws significantly raise the bar on security and privacy controls for healthcare facilities. Because this is a new law, the AC-CPO is working with County Counsel to determine its effect on the County and our operations.

On January 1, 2008, AB 1298 became law that requires covered entities to identify the types of computerized health information they maintain and explain why it must be preserved. Departments must limit collection and retention of protected data to reduce the risk of potential security breaches. HIPAA requires a six-year record retention period; departments must encrypt medical, health insurance, and confidential information covered by security breach notification laws. Because the County is subject to HIPAA notification regulations and the State has specific requirements that depend on the activity or information compromised, departments must train personnel in breach notification laws. The covered departments receive training on HIPAA and County standards in the event there is a breach involving PHI.

On January 1, 2007, AB 3013 became law and amended the State's Confidentiality of Medical Information Act to better conform to HIPAA's confidentiality provisions. In general, the law authorizes health care providers to disclose to family members or close personal friends the medical information directly relevant to that person's care and involvement. The covered entity must obtain the patient's authorization or reasonably infer, using professional judgment that the patient does not object to the disclosure.

Summary and Conclusion

Open communication and training is critical in ensuring compliance with HIPAA, State privacy laws, and County policies. Training workforce members on HIPAA and departmental privacy policies and procedures is essential to safeguarding PHI. We encourage the covered departments to timely and routinely inform the AC-CPO about privacy complaints and privacy breaches. Further, we remind covered and MOU departments to document complaints and their resolution, provide suitable training and materials to workforce members, and while we are in the interim phase for the LMS HIPAA program to be fully operable, document employee training according to HIPAA and County guidelines.

Overall the County's HIPAA program continues to advance awareness of health privacy matters. The Auditor-Controller Chief Privacy Officer is responsive to departments, constituents, workforce members, the Office for Civil Rights, and other agencies, and advises them in resolving HIPAA issues. We will continue to address areas of weakness as they are discovered through audits, employee vigilance, and complaints.

If you have questions please call me, or your staff may contact Linda T. McBride, AC-CPO, at (213) 974-2166.

WLW:KZR:LTM

c: William T Fujioka, Chief Executive Officer, Chief Executive Office
Sheila Shima, Deputy Chief Executive Officer, Chief Executive Office
Raymond G. Fortner, Jr., County Counsel
Stephanie Jo Farrell, Senior Deputy, County Counsel
Jonathan E. Fielding, M.D., Director, Department of Public Health
John F. Schunhoff, Ph.D., Interim Director, Department of Health Services
Robert Pittman, Chief Security Officer, Chief Information Office
Michael J. Henry, Director, Department of Human Resources
Dr. Marvin J. Southard, Director, Department of Mental Health
Leroy D. Baca, Sheriff, Sheriff's Department
Robert B. Taylor, Chief Probation Officer, Probation Department
Tom Tindall, Director, Internal Services Department